

## 2-GHz clock quantum key distribution over 260 km of standard telecom fiber

Shuang Wang,<sup>1</sup> Wei Chen,<sup>1</sup> Jun-Fu Guo,<sup>2</sup> Zhen-Qiang Yin,<sup>1</sup>

Hong-Wei Li,<sup>1</sup> Zheng Zhou,<sup>1</sup> Guang-Can Guo,<sup>1</sup> and Zheng-Fu Han<sup>1</sup>

<sup>1</sup>Key Laboratory of Quantum Information, University of Science and Technology of China, CAS, Hefei 230026, China

<sup>2</sup>Anhui Askay Quantum Technology Co., Ltd., Wuhu 241002, China

We report a demonstration of quantum key distribution (QKD) over a standard telecom fiber exceeding 50 dB in loss and 250 km in length. The differential phase shift QKD protocol was chosen and implemented with 2 GHz system clock rate. By careful optimization of the 1-bit delayed Faraday-Michelson interferometer and the use of the super-conducting single photon detector (SSPD), we achieved a quantum bit error rate below 2% when the fiber length was no more than 205 km, and of 3.45% for the 260 km length fiber with 52.9 dB loss. We also improved the quantum efficiency of SSPD to obtain high key rate for 50 km length.

Quantum key distribution (QKD) enables two remote participants to share unconditionally secure keys based on the principles of quantum physics [1–3]. Combined with one-time pad encryption, QKD is hopeful to effectively end the cat and mouse game between the guardians of secrets and their enemies [4], and has become one of the most dynamic research fields. After the past two decades of developments, experimental QKD has achieved significant improvements, the transmission distance from 32 cm [5] to 250 km [6], the speed (or system clock rate) from 200 Hz [5] to 10 GHz [7–9].

With the dispersion-shifted fiber, Takesue et al. realized the first QKD experiment over 42.1 dB channel loss and 200 km of distance [8]. Then, with the ultra low loss fiber, Stucki et al. implemented the first QKD experiment over 250 km of distance, but the channel loss is still 42.6 dB [6]. In this letter, focused on the transmission over the widely used standard (ITU-T G.652) telecom fiber, of which loss coefficient is about 0.2 dB/km and dispersion is about 17 ps/(km · nm) at 1550 nm region, we report a QKD experiment over 260 km of this standard telecom fiber with 52.9 dB channel loss. This is the first QKD experiment exceeding 50 dB in channel loss and 250 km in length.

We chose the differential phase shift QKD (DPS-QKD) protocol [10] to be implemented with 2 GHz rate. The experimental setup is outlined in Fig. 1, including the transmitter – Alice, quantum channel, and receiver – Bob. At Alice's site, a continuous wave (CW) laser, whose central wavelength is 1560.2 nm, is first modulated into a pulse train by an intensity modulator (IM). The phase modulator (PM) randomly encodes  $\{-\frac{\pi}{2}, \frac{\pi}{2}\}$  on each pulse, and the followed variable attenuator (VA) attenuates the average photon number per pulse to the optimal value. Alice's pattern generator (PG) has three outputs – narrow pulse with 2 GHz rate to IM, pseudo-random data to PM and 0.5 MHz sync signals to Bob. The quantum channel is the standard telecom fiber (STF). A 3-port optical circulator (CIR) at Bob's site is put before his 2-GHz, 1-bit delayed Faraday-Michelson interferometer (FMI), which makes one pulse interfere with pulses before and after it. The two outputs of the FMI are connected with a double-channel super-

conducting single photon detector (SSPD), of which D0 channel clicks if the phase difference between two adjacent pulses is 0, D1 channel clicks if the phase difference is  $\pi$ . Both sync signals and electrical pulses from SSPD are sent to the time-to-digit convertor (TDC). Once TDC records a click event, Bob and Alice can share one sifted key bit. Note that although we transmitted the sync signal via a cable in the lab, the best way to transmit the sync signal is over the quantum channel.

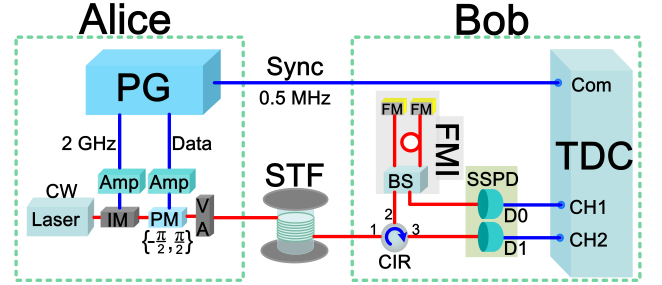


FIG. 1: (Color online) Schematic of the DPS-QKD setup.

Suppose the insertion loss (IL) of Bob's detection setup and the effective detection efficiency (EDE) of SSPD are  $\alpha_{IL}$  and  $\eta_D$ , the overall transmission and detection efficiency between Alice and Bob can be expressed as [11]

$$\eta = \eta_D \cdot 10^{-\frac{\alpha \cdot l + \alpha_{IL}}{10}}, \quad (1)$$

here  $\alpha$  and  $l$  are the loss coefficient and the length of the fiber respectively. Let  $\mu$  denote the average photon number per pulse set by Alice, the probability that one click event happens is given by

$$p_{click} \approx p_{signal} + p_{dark}, \quad (2)$$

where the signal contribution is  $p_{signal} = 1 - e^{-\mu\eta}$ , the dark count contribution is  $p_{dark} = 2 \cdot D \cdot t_w$ , here  $D$  is the dark count rate (DCR) of Bob's detector, and  $t_w$  is the measurement time window of the system [12]. Considering the dead time of the detection system  $t_d$ , the sifted key rate could be expressed as [13]

$$R_{sifted} = f \cdot p_{click} \cdot e^{-f \cdot p_{click} \cdot t_d}, \quad (3)$$

where  $f$  is the repetition rate of transmission. If the probability that a signal hit the wrong detector is  $e_s$ , which is the baseline system error rate [12], the quantum bit error rate (QBER) is given by

$$e = \frac{e_s \cdot p_{\text{signal}} + e_d \cdot p_{\text{dark}}}{p_{\text{click}}}, \quad (4)$$

where  $e_d = 0.5$  means the dark count contribution is random. Finally, the secure key rate under general individual attacks is given by [14]

$$R_{\text{secure}} = R_{\text{sifted}} \cdot \{\tau - f(e) \cdot H_2(e)\}, \quad (5)$$

where  $\tau = -(1 - 2\mu)\log_2[1 - e^2 - (1 - 6e)^2/2]$  is the compression factor in the privacy amplification process,  $f(x)$  characterizes the efficiency of error correction algorithm, and  $H_2(x)$  is the binary Shannon entropy. In order to get a tighter security threshold [15],  $f(e)$  in this paper was chosen as 1.2. Using equations from (1) to (5), we can maximize the secure key rate by setting optimal  $\mu$  for the specific experimental setup.

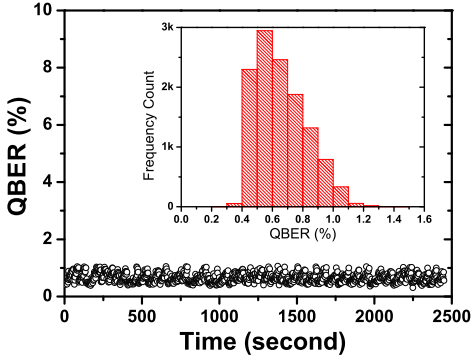


FIG. 2: (Color online) Quantum bit error rate (QBER) without phase modulation and active compensation.

Bob's experimental setup includes three main parts – the Faraday-Michelson interferometer, the superconducting single photon detector, and the time-to-digit convertor. (i) One 50/50 beam splitter (BS) and two Faraday mirrors (FM) constitute FMI, the Faraday mirror which is a combination of a 45 degree Faraday rotator and an ordinary mirror could automatically compensate for any birefringence effect in fiber [16], so the 2-GHz, 1-bit delayed FMI is almost insensitive to polarization. The interferometer was insulated from the environment and actively compensated by piezoelectric ceramics for better interference. Without phase modulation and active compensation, the mean QBER was about 0.65% over 2450 seconds (Fig. 2). However, when we added random phase modulation signal on the phase modulator, QBER increased to 1.80%, which was the value of  $e_s$  in equation (4). The IL of Bob's detection setup is about 1.5 dB, including the IL of CIR (from port 1 to port 2) and FMI.

(ii) The double-channel SSPD was made by Scontel Ltd. from Russia, and worked with a refrigeration system [17] which could obtain a temperature of 1.7 K. The detector had a counting rate more than 70 MHz, and a jitter value better than 50 ps. By carefully increasing the bias current, we achieved 3.0% average quantum efficiency with 1 Hz DCR. (iii) The TDC not only recorded the sync and SSPD signals, but also set the measurement time window  $t_w$  during the experiment. The value  $t_w$  was set to 200 ps, and this set reduced the quantum efficiency by 17%. The dead time of TDC is 15 ns, which is the value of dead time of the whole detection system.

Based on these specific experimental parameters, the secure key rate under individual attacks could be maximized by choosing optimal  $\mu$  for each fiber length, and the attainable maximum distance is 281 km (with 0.2 dB/km loss coefficient) in principle (Blue dot line in Fig. 3). With standard telecom fiber, the sifted key rates and QBERs were measured at seven different fiber lengths – 10 km, 50 km, 75 km, 100 km, 150 km, 205 km, and 260 km. We set  $\mu = 0.19$  for 10 km and 50 km fiber length, and  $\mu = 0.20$  for other length values.

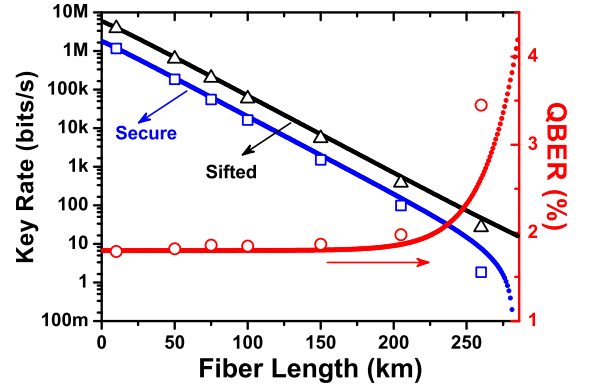


FIG. 3: (Color online) Experimental results of DPS-QKD.

The dark count rate of detectors is a major limiting factor for long-distance QKD [6]. Therefore the ultra low-noise SSPD was used in our DPS-QKD system. We first set the EDE and DCR of SSPD at 2.5% and 1 Hz respectively, and the measurement results were shown as open shapes in Fig. 3. For each data, we ran the QKD process ten times, and each run lasted ten minutes. The measured QBERs and sifted key rates are the average values of the ten runs, but secure key rates are calculated results by equation (5). Through careful optimization of the 1-bit delayed interferometer, we achieved the values of QBER below 2% for the first six lengths, and of 3.45% for the 260 km length fiber with 52.9 dB loss (Red open circles in Fig. 3). At 10 km and 50 km fiber length, 1.16 Mbits/s and 185 kbits/s secure key rate under individual attacks were achieved. At 205 km with 41.6 dB transmission loss, 99.2 bits/s secure key rate was obtained, this

rate value was more than eight times of that achieved in 10-GHz DPS-QKD experiment at 200 km with 42.1 dB loss [8]. Although the channel loss of 260 km was one order of magnitude larger than the loss 42.6 dB in previous 250 km QKD experiment [6], in which the ultra low loss fiber with 0.164 dB/km loss coefficient was used, secure keys with 1.85 bits/s rate could still be shared between Alice and Bob.

When the transmission fiber length was short, the signal contribution  $p_{\text{signal}}$  was much larger than the dark count contribution  $p_{\text{dark}}$ . In order to get higher key rate, we improved the quantum efficiency of SSPD by increasing the bias current, though the dark count rate increased faster as the current increased. In the 50 km fiber length experiment, another  $\eta_D = 11.2\%$  value was tested, QBER was 1.89%, and the corresponding secure key rate got up to 0.81 Mbits/s, which was close to Dixon's BB84 experiment [18].

For the QKD system over long distance, the nonzero accumulated chromatic dispersion of standard telecom fiber would severely limit the performance of QKD, especially for gigahertz systems [19]. The optical pulses are broadened during propagation through the optical fiber, so photons would spread outside the measurement time window, which reduces the effective quantum efficiency, and even overlap with photons of neighbor pulses, which degrades the encoded signal. Take the 10-GHz QKD system for example, in which pulses are separated by 100 ps,

while the dispersion is up to 153 ps after propagating in 25 km single mode fiber [12], so the dispersion-shifted fiber was used in [7] and [8]. In our experiment, the full width at half maximum of the 2-GHz pulse train was 170 ps, this wide width limited the effects of chromatic dispersion to some extent. Fig. 3 shows that the measured sifted key rates (or counting rates) deviate from the simulation results, and the reduction increases as the fiber length increases. At 205 km transmission distance, the measured sifted key rate was 69.1% of the simulation one. The transmission loss 41.6 dB was higher than  $0.2 \times 205$  dB, and the set average photon number 0.20 was a little bit larger than the optimum one (0.19776). After removing effects of these differences, there was still 20.8% reduction. The chromatic dispersion of the fiber was the main cause of this reduction.

In summary, we have experimentally demonstrated that quantum key distribution is possible over 260 km standard telecom fiber with 52.9 dB loss. Using the ultra low loss fiber with 0.164 dB/km loss coefficient [6], the quantum key exchange over 340 km distance is in sight.

This work was supported by the National Basic Research Program of China (Grants No. 2011CBA00200 and No. 2011CB921200), National Natural Science Foundation of China (Grant No. 60921091), and National High Technology Research and Development Program of China (863 program) (Grant No. 2009AA01A349).

- 
- [1] C. H. Bennett and G. Brassard, Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE, 1984), p. 175.
  - [2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
  - [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301(2009).
  - [4] D. J. Rogers, "Broadband Quantum Theory," (Morgan & Claypool, 2010).
  - [5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology, **5**, 3 (1992)
  - [6] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).
  - [7] H. Takesue, E. Diamanti, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **14**, 9522 (2006).
  - [8] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto, Nature Photonics **1**, 343 (2007).
  - [9] I. Choi, R. J. Young, and P. D. Townsend, New J. Phys. **13**, 063039 (2011).
  - [10] K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
  - [11] X. F. Ma, B. Qi, Y. Zhao, and H. K. Lo, Phys. Rev. A **72**, 012326 (2005).
  - [12] E. Diamanti, "Security and implementation of differential phase shift quantum key distribution systems," Ph.D. thesis, Stanford University (2006).
  - [13] E. Diamanti, H. Takesue, C. Langrock, M. M. Fejer, and Y. Yamamoto, Opt. Express **14**, 13073 (2006).
  - [14] E. Waks, H. Takesue, and Y. Yamamoto, Phys. Rev. A **73**, 012344 (2006).
  - [15] Q. Zhang, H. Takesue, T. Honjo, K. Wen, T. Hirohata, M. Suyama, Y. Takiguchi, H. Kamada, Y. Tokura, O. Tadanaga, Y. Nishida, M. Asobe, and Y. Yamamoto, New J. Phys. **11**, 045010 (2009).
  - [16] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).
  - [17] G. Goltsman, A. Korneev, A. Divochiy, O. Minaeva, M. Tarkhov, N. Kaurova, V. Seleznev, B. Voronov, O. Okunev, A. Antipov, K. Smirnov, Yu. Vachtomin, I. Milostnaya, and G. Chulkova, J. Mod. Opt. **56**, 1670 (2009).
  - [18] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, Appl. Phys. Lett. **96**, 161102 (2010).
  - [19] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, New J. Phys. **11**, 045019 (2009).